Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently amended) A computer-implemented method for transmitting a message from a sender to an intended recipient comprising:

encrypting a message using a symmetric key;

sending the encrypted message to an intended recipient without making the symmetric key immediately accessible to the intended recipient;

providing the symmetric key to a third party; and

if the intended recipient signs and returns to the third party a receipt for the message, transferring, by the third party, the receipt to ~~the~~ a sender and providing the symmetric key to the intended recipient.

2. (Currently amended) The computer-implemented method of claim 1 wherein the receipt signed by the recipient contains an identifier computed from the message and the symmetric key using cryptographically secure hash functions.

3. (Currently amended) A computer-implemented method for transmitting a message from a sender to an intended recipient comprising:

at ~~the~~ a sender, encrypting a message using a symmetric key, encrypting the symmetric key to make the symmetric key accessible to a third party but not immediately accessible to an intended recipient and sending the encrypted message and the encrypted symmetric key to ~~an~~ the intended recipient;

at the recipient, signing a receipt for the message and sending the receipt and the encrypted symmetric key to the third party; and

at the third party, transferring the receipt to the sender and providing the symmetric key to the intended recipient if the receipt is properly signed.

4. (Currently amended) A computer-implemented method for certifying receipt of a message, the message being sent from a sender to an intended recipient and being encrypted by a symmetric key~~, the symmetric key being encrypted to be only accessible to the third party~~, and the method executing at a third party distinct from the sender and the recipient, the method comprising:

receiving a signed receipt and ~~the~~ an encrypted symmetric key from an intended recipient, the signed receipt memorializing receipt of the encrypted message by the intended recipient;

verifying the signed receipt;

transferring the verified receipt to ~~the~~ a sender; and

providing the symmetric key to the intended recipient.

5. (Currently amended) A computer-implemented method for certifying receipt of a message, the message being sent from a sender to an intended recipient and being encrypted by a symmetric key~~, the message including a separately encrypted message header including the symmetric key and a message identifier associated with the message~~, the method executing at a third party distinct from the sender and the recipient, the method comprising:

receiving a separately encrypted message header associated with the message and a certified receipt originating from ~~the~~ an intended recipient, the certified receipt including a~~the~~ message identifier signed by the intended recipient;

decrypting the separately encrypted message header to expose ~~the~~ a symmetric key and the message identifier;

verifying the certified receipt including verifying the signature of the intended recipient and the message identifier in the certified receipt is the same as the message identifier obtained from the separately encrypted message header;

forwarding the certified receipt to the sender; and

forwarding the symmetric key to the intended recipient.

6. (Currently amended) A computer-implemented method for transmitting a message from a sender to an intended recipient comprising:

encrypting a message using a symmetric key;

storing the symmetric key and the message;

sending the encrypted message to an intended recipient without the symmetric key;

forwarding the encrypted symmetric key to a third party; and

receiving from the third party a certified receipt verified by the third party indicating receipt of the message by the intended recipient.~~; and~~

~~verifying the validity of the certified receipt using the stored symmetric key and the certified message~~

7. (Currently amended) A computer-implemented method for transmitting a message from a sender to an intended recipient comprising:

identifying a message for transmission to an intended recipient;

creating a message header that includes a symmetric key and a message identifier associated with the message;

encrypting the message using the symmetric key;

public key encrypting the message header using a public key of a third party;

attaching the message header to the encrypted message forming a certified message and forwarding the certified message to the intended recipient;

storing a copy of the certified message and the symmetric key;

receiving a certified receipt originating from ~~the~~ an intended recipient, the certified receipt being verified at the third party and forwarded to the sender after verification; and

verifying ~~the~~ validity of the receipt using the stored symmetric key and the certified message.

8. (Currently amended) A computer-implemented method for providing a receipt for a message, the message being sent from a sender to an intended recipient and the method executing at the recipient, the method comprising:

receiving an encrypted message from ~~a~~the sender, the message encrypted by a symmetric key;

creating a receipt for the encrypted message including signing a hash of the encrypted message and returning the signed receipt to a third party; ~~and~~

after verification of the signed receipt at the third party, receiving the symmetric key from the third party; and

~~so that the intended recipient can~~ decrypting the encrypted message using the symmetric key.

9. (Currently amended) The computer-implemented method of claim 8 wherein the step of receiving the symmetric key includes not receiving the symmetric key until a successful transfer of the signed receipt to the sender.

10. (New) The method of claim 6, further comprising:

verifying the validity of the certified receipt using the stored symmetric key and the certified message.

11. (New) A computer-implemented method for computing a message identifier associated with a message without exposing the content of the message to a third party, comprising:

receiving a message encrypted by a symmetric key;

receiving a hash of the symmetric key;

generating a representation of the hash of the symmetric key and the message encrypted by the symmetric key; and

sending the message identifier along with an associated message to an intended recipient of the message, the message identifier able to be viewed by a third party to verify receipt of the message at the intended recipient without exposing the message content to the third party.

12. (New) The computer-implemented method of claim 11, wherein:

generating the representation of the hash of the symmetric key and the message encrypted by the symmetric key includes using a hash function.

13. (New) The computer-implemented claim 11, further comprising:

receiving the message identifier at the intended recipient;

generating a receipt including the message identifier, at the intended recipient; and

sending the receipt to the third party.

14. (New) The computer-implemented claim 13, further comprising:

receiving the receipt;

verifying the receipt without accessing the message content; and

providing the receipt to a sender.

15. (New) The computer-implemented claim 11, further comprising:

encrypting the message with the symmetric key prior to sending; and

sending the symmetric key to the intended recipient from the third party so that the intended recipient can decrypt the message.

16. (New) The computer-implemented claim 11, further comprising:

sending the encrypted symmetric key to the intended recipient with the message;

at the intended recipient, sending the encrypted symmetric key to the third party with the receipt; and

sending the receipt to a sender after verification of the receipt.

17. (New) A computer-implemented method for generating a signed receipt associated with a message without exposing the content of the message to a third party, comprising:

receiving a message encrypted by a symmetric key;

receiving a hash of the symmetric key;

generating a representation of the hash of the symmetric key and the message encrypted by the symmetric key;

signing the representation to generate a signed receipt; and

sending the signed receipt to a third party for transfer to a sender.

18. (New) The computer-implemented method of claim 17, further comprising:

verifying the validity of the signed receipt at the third party.

19. (New) The computer-implemented method of claim 18, further comprising:

allowing a recipient access to the content of the message if the signed receipt is verified at the third party.

20. (New) A computer-implemented method for time-stamping a message without exposing the content of the message to a time stamping authority, comprising:

encrypting the message using a symmetric key;

computing a hash of the symmetric key;

generating a representation of the hash of the symmetric key and the message encrypted by the symmetric key; and

time-stamping the representation.

21. (New) The computer-implemented method of claim 20, wherein:

time-stamping the representation includes sending the representation to a time-stamping authority and receiving from the time-stamping authority a time stamp certificate including the representation and a time.

22. (New) The computer-implemented method of claim 20, wherein:

time-stamping the representation includes sending the representation to a time-stamping authority and receiving from the time-stamping authority a time stamp certificate including the representation, a time, a sender identification and a recipient identification for the message.

23. (New) The computer-implemented method of claim 20, wherein:

time-stamping the representation includes sending the representation to a time-stamping authority and receiving from the time-stamping authority a time stamp certificate including the representation, a time, a sender identification and a recipient identification for the message and at least one of a public key of the sender and a public key of the recipient.

24. (New) A computer-implemented method for generating a signed receipt certifying that a message has been received at a particular time by an intended recipient, without exposing the message content to a third party, comprising:

receiving a message encrypted by a symmetric key;

receiving a hash of the symmetric key;

generating a representation of the hash of the symmetric key and the message encrypted by the symmetric key;

time-stamping the representation;

signing the time-stamped representation; and

sending the time-stamped representation to a third party such that the time stamp can be verified by the third party without exposing the content of the message to the third party.

25. (New) The computer-implemented method of claim 24, further comprising:

verifying the validity of the signed receipt at the third party.

26. (New) The computer-implemented method of claim 25, further comprising:

allowing an intended recipient access to content of the message if the signed receipt is verified at the third party.

27. (New) A computer-implemented method for generating a signed receipt for a message certifying a sending time and a receiving time by an intended recipient without exposing the content of the message to a third party, comprising:

receiving a message encrypted with a symmetric key;

receiving a hash of the symmetric key;

receiving a time-stamped representation of the hash of the symmetric key and the encrypted message, the representation being time-stamped at time of sending;

time-stamping the representation at a time of receiving;

combining the representation time-stamped at the time of sending and the representation time-stamped at the time of receiving providing a combined receipt; and

signing the combined receipt; and

sending the combined receipt to a third party such that the combined receipt can be verified by the third party without exposing the content of the message to the third party.

28. (New) The computer-implemented method of claim 27, further comprising:

verifying the validity of the signed receipt at the third party.

29. (New) The computer-implemented method of claim 27, further comprising:

allowing an intended recipient access to content of the message if the signed receipt is verified at the third party.